Defining Cyber Discovery: From Preparation to Response*

Preparation
Initiation of the Cyber Discovery Process

- Cyber Discovery Goals
- Data Collection and Ingestion
- Data Exploration
- Data Processing

Planning
Model and Protocol Planning

- Model and Protocol Planning (AI + Experts)

Training
Selection, Building, Testing, and Training

- Model and Protocol Selection And Building
- Model and Protocol Testing and Training

Tuning
Validation and Evaluation

- Model and Protocol Validation
- Model and Protocol Evaluation

Discovery
Adaptation, Deployment, and Maintenance

- Model and Protocol Adaptation (Adjustment)
- Model and Protocol Deployment (Execution)
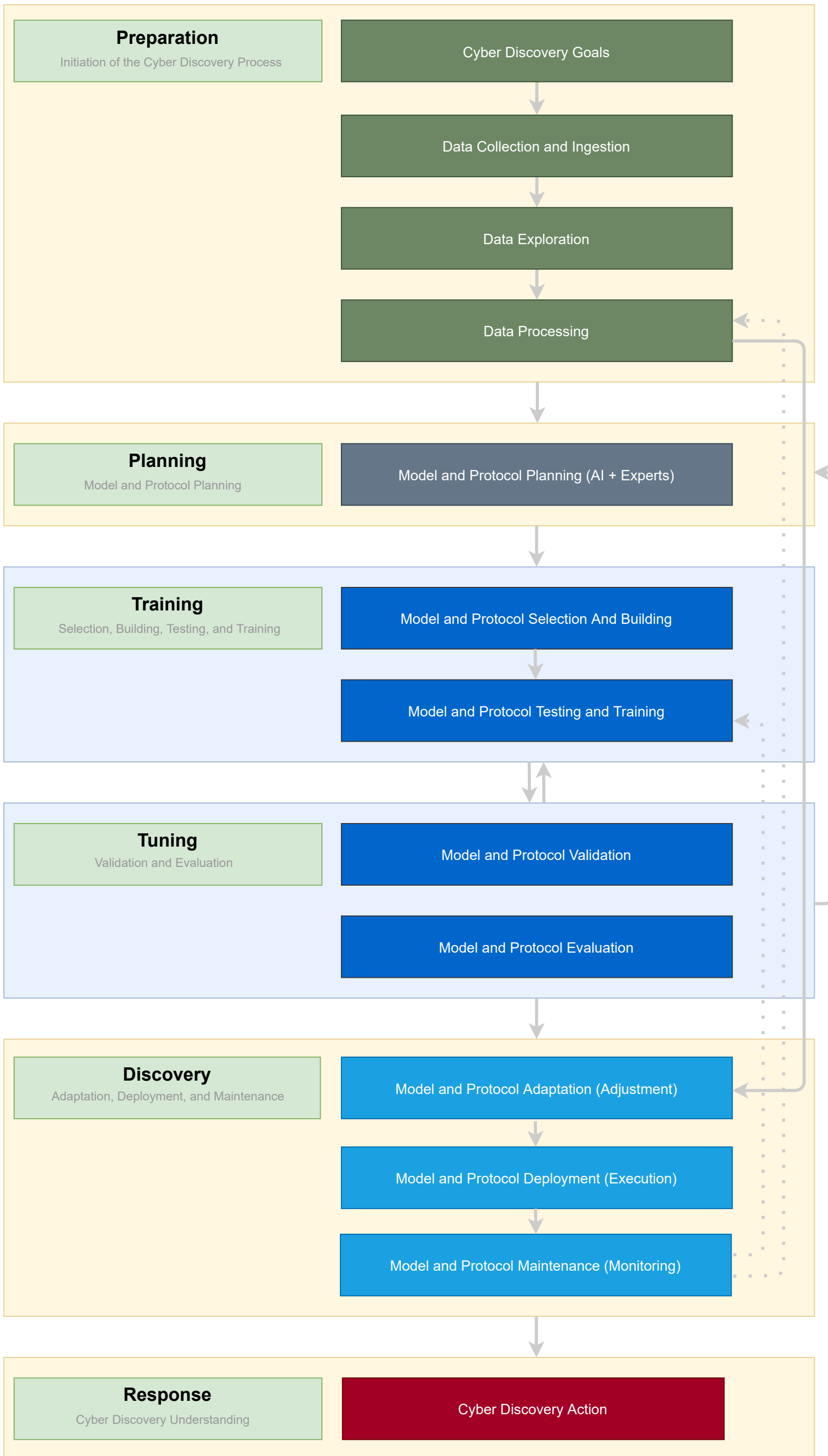- Model and Protocol Maintenance (Monitoring)

Response
Cyber Discovery Understanding

- Cyber Discovery Action

*Generic Cyber Discovery Reference Model: Modified from AI Lifecycle Generic Reference Model (European Agency For Cybersecurity (ENISA) Report *AI Cybersecurity Challenges - Threat Landscape for Artificial Intelligence* - 2021)